

RECEIVED
CENTRAL FAX CENTER

AUG 25 2005

DILLON & YUDELL LLP
ATTORNEYS AT LAW

USPTO FACSIMILE TRANSMITTAL SHEET

TO:	FROM:	
Examiner Jenise E. Jackson	Andrew J. Dillon, Reg. No. 29,634	
ORGANIZATION:	DATE:	
US Patent and Trademark Office	August 25, 2005	
ART UNIT:	CONFIRMATION NO.:	TOTAL NO. OF PAGES INCLUDING COVER:
2131		13
FAX NUMBER:	APPLICATION SERIAL NO.:	
571-273-8300	09/847,085	
ENCLOSED:	ATTORNEY DOCKET NO.:	
Appeal Brief	RPS920000109US1	

☒ URGENT ☐ FOR REVIEW ☐ PLEASE COMMENT ☐ PLEASE REPLY ☐ PLEASE RECYCLE

NOTES/COMMENTS:

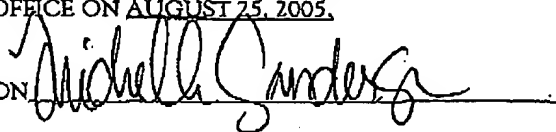
RECEIVED
OIPE/IAP

AUG 26 2005

CERTIFICATE OF FACSIMILE TRANSMISSION UNDER 37 C.F.R. § 1.8(A)

I HEREBY CERTIFY THAT THIS CORRESPONDENCE IS BEING FACSIMILE TRANSMITTED TO
THE U.S. PATENT AND TRADEMARK OFFICE ON AUGUST 25, 2005.

SIGNATURE OF MICHELLE SANDERSON



This fax from the law firm of Dillon & Yudell LLP contains information that is confidential or privileged, or both. This information is intended only for the use of the individual or entity named on this fax cover letter. Any disclosure, copying, distribution or use of this information by any person other than the intended recipient is prohibited. If you have received this fax in error, please notify us by telephone immediately at 512.343.6116 so that we can arrange for the retrieval of the transmitted documents at no cost to you.

8911 N. CAPITAL OF TEXAS HWY., SUITE 2110, AUSTIN, TEXAS 78759
512.343.6116 (V) • 512.343.6446 (F) • DILLONYUDELL.COM

RECEIVED
CENTRAL FAX CENTER

AUG 25 2005

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

IN RE APPLICATION OF:
DARYL CARVIS CROMER ET AL.
SERIAL NO.: 09/847,085
FILED: MAY 2, 2001
FOR: DATA PROCESSING SYSTEM
AND METHOD FOR
PASSWORD PROTECTING A
BOOT DEVICE

§ ATTY. DOCKET NO.: RPS920000109US1
§
§
§ EXAMINER: JENISE E. JACKSON
§
§
§
§ ART UNIT: 2131
§
§
§
§
§

APPEAL BRIEF UNDER 37 C.F.R. §1.192

Mail Stop Appeal Briefs - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Brief is submitted in support of the Appeal of the Examiner's final rejection of Claims 1-16 in the above-identified application. A Notice of Appeal was filed in this case on July 29, 2005 and received in the United States Patent and Trademark Office on July 29, 2005. Please charge the fee of \$500.00 due under 37 C.F.R. §1.17(c) for filing the brief, as well as any additional required fees, to **Lenovo Deposit Account No. 50-3533**.

Certificate of Transmission/Mailing

I hereby certify that this correspondence is being facsimile transmitted to the USPTO at 571-273-8300 or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to:
Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450 on the date shown below.

Typed or Printed Name: Michelle Sanderson

Date:

8/25/05

Signature:

Michelle Sanderson

RPS920000109US1US1

Appeal Brief

Serial No. 09/847,085

08/26/2005 GWORDOF1 00000034 503533 09847085

- 1 -

01 FC:1402 500.00 DA

REAL PARTY IN INTEREST

The real party in interest in the present Application is International Business Machines Corporation, the Assignee of the present application as evidenced by the Assignment set forth at reel 011790, frame 0911.

RELATED APPEALS AND INTERFERENCES

There are no Appeals or Interferences known to Appellants, the Appellants' legal representative, or assignee, which would be directly affected or have a bearing on the Board's decision in the present Appeal.

STATUS OF CLAIMS

Claims 1-16 stand finally rejected by the Examiner as noted in the Final Action dated May 18, 2005. Claims 17-19 are cancelled.

STATUS OF AMENDMENTS

No amendments to the claims have been made subsequent to the final rejections that lead to this appeal.

SUMMARY OF THE CLAIMED SUBJECT MATTER

Appellants' Claim 1 recites a method in a data processing system for maintaining security during booting of the data processing system (Specification, page 4, lines 1-10, Figures 2A-2B). During a boot process, a boot device is interrogated for password information (page 4, lines 4-5, Figure 2A). In response to the boot device supplying password information corresponding to that of a trusted boot device, the data processing system is booted utilizing the boot device, where the booting includes booting the data processing system utilizing the boot device without entry of password information corresponding to that of a trusted boot device by a human user (page 4, lines 5-10, Figures 2A-2B).

RPS920000109US1US1

Appeal Brief

Serial No. 09/847,085

- 2 -

Appellants' Claim 7 recites a data processing system including a boot device (page 4, lines 1-10, Figure 1), a processor (page 6, line 9, Figure 1), and a memory coupled to the processor for communication (page 6, lines 10-12, Figure 1). The memory includes startup software that, when executed by the processor during the boot process, interrogates the boot device for password information and, responsive to the boot device supplying password information corresponding to that of a trusted boot device, boots the data processing system utilizing the boot device, wherein the startup software boots the data processing system utilizing the boot device without entry of the password information corresponding to that of a trusted boot device by a human user (page 4, lines 5-10, Figures 2A-2B).

Appellants' Claim 12 recites a program product that includes a computer-usable medium (page 11, lines 10-15) and startup software encoded within the computer-usable medium, wherein the startup software causes a data processing system to interrogate a boot device for password information during a boot process, and responsive to the boot device supplying password information corresponding to that of a trusted boot device, to boot the data processing system utilizing the boot device without entry of any password information corresponding to that of a trusted boot device by a human user (page 4, lines 5-10, Figures 2A-2B).

Appellants' Claim 4 recites a method for interrogating a plurality of boot devices for password information by interrogating a plurality of boot devices in sequence according to a priority order until a boot device supplies password information corresponding to that of a trusted boot device (page 9, lines 13-20, Figures 2A-2B).

Appellants' Claim 9 recites a data processing system having a plurality of boot devices, wherein startup software interrogates the plurality of boot devices for password information in sequence according to priority order until a boot device supplies password information corresponding to that of a trusted boot device (page 9, lines 13-20, Figures 2A-2B).

Appellants' Claim 14 recites a program product stored in a computer-readable medium for interrogating a plurality of boot devices for password information by interrogating a plurality of boot devices in sequence according to a priority order until a boot device supplies password information corresponding to that of a trusted boot device (page 9, lines 13-20, Figures 2A-2B).

GROUND OF REJECTION TO BE REVIEWED ON APPEAL

- I. The Examiner's rejection of Appellants' Claims 1-3, 7-8, 12-13 under 35 U.S.C. § 102(b) as being anticipated under *Pearce et al.* (U.S. Patent No. 6,484,308) is to be reviewed on Appeal.
- II. The Examiner's rejection of Appellants' Claims 4, 9, and 14 under 35 U.S.C. § 103(a) as being unpatentable over *Pearce* in view of *Herzi et al.* (U.S. Patent No. 6,353,885) is to be reviewed on Appeal.

ARGUMENT

- I. The rejection of Appellants' Claims 1-3, 7-8, 12-13 under 35 U.S.C. § 102(b) as being anticipated under *Pearce*:

In the Examiner's Final Action, Claims 1-3, 7-8, 12-13 were rejected under 35 U.S.C. § 102(b) as being anticipated by *Pearce*. The Examiner's rejection should be reversed because *Pearce* does not teach or suggest each claimed feature.

Regarding exemplary Claim 1, *Pearce* does not teach or suggest "interrogating a boot device for password information" and "in response to the boot device supplying password information corresponding to that of a trusted boot device, booting the data processing system utilizing the boot device".

Figure 3 of *Pearce* is a high-level flowchart diagram illustrating the disclosed system boot procedure. As indicated by blocks 302, 304, and 306, the "system boot" procedure includes powering on the hard drive, reading the drive identification information from the hard drive, and storing the drive identification. Later, after the system has been booted from the disk drive with the stored identification, the system may be placed into a "suspend state and/or the hard drive may be powered down" (col. 4, lines 58-60). On resume, the system does not have to be restarted or "booted", but resumes, as depicted in Figure 6, which involves the system reading the drive information from the hard disk drive currently installed in the system and comparing

the drive information with the set of drive information stored in memory (blocks 602, 604, and 606). If the drive information of the currently installed drive matches the drive information stored in memory, the system resumes operation. If not, the system notifies the user that the currently installed drive is not the expected drive and powers down (blocks 608, 614, 615, and 616).

As depicted in Figures 3 and 6, the system disclosed in *Pearce* does not make *any* determination of whether or not the hard drive ("boot device") is a trusted boot device during the *booting process*. In fact, *any* hard drive can be utilized to boot the system disclosed in *Pearce*. *Pearce's* determination of whether or not the installed hard drive is a trusted boot device (whether the installed hard drive is the same as the one used to boot the system) does not occur until the "hard drive resumes", as illustrated in Figure 6. Therefore, nothing in *Pearce* teaches or suggests "interrogating a boot device for password information" and "*in response to the boot device supplying password information corresponding to that of a trusted boot device, booting the data processing system utilizing the boot device*" (emphasis added).

Accordingly, in light of the preceding argument, Appellants believe that independent Claims 1, 7, and 12 and all dependent claims are not anticipated by *Pearce* and are thus not rendered unpatentable.

II. The rejection of Appellants' Claims 4, 9, and 14 under 35 U.S.C. § 103(a) as being unpatentable over *Pearce* in view of *Herzi*:

In Examiner's Final Action, Claims 4, 9, and 14 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Pearce* in view of *Herzi*. The Examiner's rejection should be reversed because *Pearce* in view of *Herzi* does not teach or suggest each claimed feature.

Regarding exemplary Claim 4, nothing in *Pearce* in view of *Herzi* teaches or suggests "interrogating a plurality of boot devices in sequence according to a priority order until a boot device supplies password information corresponding to that of a trusted boot device".

Herzi discloses a system and method of easily configuring a computer system BIOS firmware by utilizing a smart card (col. 4, lines 40-42). Also, *Herzi* discloses booting a computer system from user-defined sources, such as a removable hard disk drive, floppy drive, or optical drive, depending on the BIOS settings on the smart card (col. 5, lines 58-64). *Herzi* discloses the booting of a computer system utilizing BIOS settings from a smart card after a user enters a personal identification number (PIN). However, nothing in *Herzi* teaches or suggests a "boot device supply[ing] password information corresponding to that of a trusted boot device" (Claim 4).

The Examiner asserts on page 5, paragraph 17 of the Final Office action mailed May 18, 2005 that *Herzi* discloses both the use of a BIOS level password (col. 5, lines 35-36) and that a user who has the BIOS password can change the configuration settings, including the ability to choose where to boot from, the floppy disk, hard drive, CD-ROM (col. 5, lines 33-48, 58-64). Even if Examiner's assertions are true, *Pearce* in view of *Herzi* does not result in the claimed invention.

For example, the PIN as disclosed in *Herzi* secures the BIOS settings on the smart card, but does not identify a "trusted boot device," as indicated in Claim 4. The BIOS settings, as Examiner asserts, allows the user to choose the boot order of the computer system components. For instance, BIOS settings allow a user to determine that a computer system should first attempt to boot from a hard disk drive, and if the hard disk drive is not present in the computer system, the computer system should look to a floppy or optical drive to complete the booting process. However, these BIOS settings and the PIN *provided by the user* only indicate that the user may access a computer system utilizing the present BIOS settings. The PIN: (1) *is not provided by a boot device* and (2) *does not identify a trusted boot device*. The PIN merely identifies the user as one who is authorized to access the computer system utilizing the specific BIOS settings store on the smart card.

Because the PIN does not identify a trusted boot device, a person with the required PIN may access the system utilizing the BIOS settings stored on the smart card and replace any of the

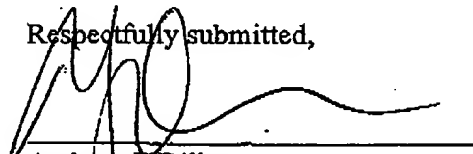
boot devices on the system (e.g., hard disk drive, floppy or optical drive, etc.) with unauthorized boot devices and still have access to the computer system.

Therefore, nothing in *Pearce* in view of *Herzi* teaches or suggests "interrogating a plurality of boot devices in sequence according to a priority order until a boot device supplies password information corresponding to that of a trusted boot device". Accordingly, Appellants believe that the arguments applicable to Claim 4 also apply to similar Claims 9 and 14. Also, even if *Herzi* teaches or suggest the claimed element, the arguments applicable to Examiner's rejection under § 102(b) also apply to Claim 4, 9, and 14 as dependent Claims to independent Claims 1, 7, and 12.

CONCLUSION

Appellants have pointed out with specificity the manifest error in the Examiner's rejections, and the claim language that renders the invention patentable over the combination of references. Appellants, therefore, respectfully request that this case be remanded to the Examiner with instructions to issue a Notice of Allowance for all pending claims.

Respectfully submitted,



Andrew J. Dillon
Reg. No. 29,634
DILLON & YUDELL LLP
8911 N. Capital of Texas Highway
Suite 2110
Austin, Texas 78759
512-343-6116

ATTORNEY FOR APPELLANTS

CLAIMS APPENDIX

1. A method in a data processing system for maintaining security during booting of the data processing system, said method comprising:
 - during a boot process, interrogating a boot device for password information; and
 - in response to the boot device supplying password information corresponding to that of a trusted boot device, booting the data processing system utilizing the boot device, wherein said booting comprises booting the data processing system utilizing the boot device without entry of any of said password information corresponding to that of a trusted boot device by a human user.
2. The method according to Claim 1, wherein said password information includes at least a serial number of the boot device.
3. The method according to Claim 1, wherein interrogating said boot device for password information comprises startup software interrogating the boot device.
4. The method according to Claim 1, wherein interrogating said boot devices for password information comprises interrogating a plurality of boot devices in sequence according to a priority order until a boot device supplies password information corresponding to that of a trusted boot device.
5. The method according to Claim 1, and further comprising:
 - storing a password in non-volatile storage of the data processing system; and
 - determining that said boot device has supplied password information corresponding to a trusted boot device by hashing password information supplied by the boot device and comparing the hashed password information with the stored password.
6. The method according to Claim 5, and further comprising obtaining said password by interrogating the boot device for the password information with a password-protected configuration routine.

7. data processing system comprising:

a boot device;

a processor; and

memory coupled to said processor for communication, said memory including startup software that, when executed by said processor during a boot process, interrogates the boot device for password information and, responsive to the boot device supplying password information corresponding to that of a trusted boot device, boots the data processing system utilizing the boot device, wherein said startup software boots the data processing system utilizing the boot device without entry of any of said password information corresponding to that of a trusted boot device by a human user.

8. The data processing system of Claim 7, wherein said password information includes at least a serial number of the boot device.

9. The data processing system of Claim 7, said data processing system having a plurality of boot devices including the boot device, wherein said startup software interrogates said plurality of boot devices for password information in sequence according to a priority order until a boot device supplies password information corresponding to that of a trusted boot device.

10. The data processing system of Claim 7, and further comprising non-volatile storage that stores a password, wherein said startup software determines that said boot device has supplied password information corresponding to a trusted boot device by hashing password information supplied by the boot device and comparing the hashed password information with the password stored in non-volatile storage.

11. The data processing system of Claim 10, said startup software including a password-protected configuration routine that obtains said password by interrogating the boot device for the password information.

12. A program product comprising:

a computer usable medium; and

startup software encoded within said computer usable medium, wherein said startup software causes a data processing system to interrogate the boot device for password information during a boot process and, responsive to the boot device supplying password information corresponding to that of a trusted boot device, to boot the data processing system utilizing the boot device, wherein said startup software boots the data processing system utilizing the boot device without entry of any of said password information corresponding to that of a trusted boot device by a human user.

13. The program product of Claim 12, wherein said password information includes at least a serial number of the boot device.

14. The program product of Claim 12, said data processing system having a plurality of boot devices including the boot device, wherein said startup software causes the data processing system to interrogate said plurality of boot devices for password information in sequence according to a priority order until a boot device supplies password information corresponding to that of a trusted boot device.

15. The program product of Claim 12, wherein said startup software determines that said boot device has supplied password information corresponding to a trusted boot device by hashing password information supplied by the boot device and comparing the hashed password information with a password stored in non-volatile storage of the data processing system.

16. The program product of Claim 15, said startup software including a password-protected configuration routine that obtains said password by interrogating the boot device for the password information.

17.-19. (canceled)

EVIDENCE APPENDIX

RPS920000109US1US1

Appeal Brief
- 11 -

Serial No. 09/847,085

RELATED PROCEEDINGS APPENDIX

RPS920000109US1US1

Appeal Brief
- 12 -

Serial No. 09/847,085